Measured Responses to Cyber Attacks Using Schmitt Analysis

Presented by

Bret Michael & Tom Wingfield

Naval Postgraduate School

Joint work with

Duminda Wijesekera

George Mason University

This research is funded by the
U.S. Department of Homeland Security

Disclaimer

- The views and conclusions contained in this presentation are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the U.S. Government.

Cyber terrorism

- "When a nation, terrorist group, or other adversary attacks the United States through cyberspace, the U.S. response need not be limited to criminal prosecution. The United States reserves the right to respond in an appropriate manner. The United States will be prepared for such contingencies."
  - U.S. President. *Critical Infrastructure Protection Board. The National Strategy to Secure Cyberspace* (Washington, D.C.: Government Printing Office, Feb. 2003).

A matter of when, not if

- Evidence exists that AlQaida and other terrorist groups are interested in conducted cyber terrorism

Countering attacks

- U.S. and other nations are developing cyber weapons to counter terrorist threats

Lawful responses to attacks

- While fashioning responses to terrorist acts, law enforcement, military, and intelligence communities need to abide by
  - U.S. domestic law
  - Those portions of international law that the U.S. recognizes

Domestic preparedness

- "Legal preparation is a vital but often overlooked aspect … [and such preparedness] affords law enforcement the necessary powers to investigate and prosecute those who possess or attempt to use" weapons of mass destruction
  - R. Pagni, Consequence management in the 1995 sarin attacks on the Japanese subway system, *Studies in Conflict and Terrorism* 25, 6 (2002).

Central legal question

- "…there is at present no conclusive legal authority for what, if any, information warfare activities would constitute 'armed attacks,' 'aggression,' or 'force' in international law."
  - R. E. Overill, How re(pro)active should an IDS be?, *Proc. First Int. Workshop on the Recent Advances in Intrusion Detection* (Louvain-la-Neuve, Belgium, Sept. 1998).

Answering the question

- "When does the attack rise to the level of a 'use of force' under international law?"
  - Ample precedent for giving finely-calibrated answers for attacks involving tradition, kinetic attacks
  - Answering this question for cyber attacks is problematic
    - Information operations (IO) involves the use of digital weapons, new methods of attack, and novel target lists

Two schools of thought

- "Common sense" approach
  - Concentrate solely on the quantum of damage done, irrespective of the means of attack
  - Out of sync with the prevailing structure of the prevailing structure of int. law (UN Charter Paradigm)
- Anything other than an armed attack is permissible
  - The quantity of force is less important than the quality of force
  - Fails to account for newly destructive capacities of IO

Need for change

- "… as the nature of a hostile act becomes less determinative of its consequences, current notions of 'lawful' coercive behavior by states, and the appropriate responses thereto, are likely to evolve accordingly."
  - M. N. Schmitt, Bellum Americanum: The U.S. view of twenty-first century war and its possible implications for the law of armed conflict, *Mich. J. Int. Law* 19, 4 (1998).

Schmitt's contribution

- Introduction of an normative framework for translating the UN Charter paradigm into its quantitative components
  - Legal equivalent of going from analog to digital
  - Way of organizing analyses in something other than a cloud of subjective uncertainty

Schmitt Analysis

- Consists of applying a fixed quantitative scale (e.g., 1 to 10) to each of seven factors in order to describe any information operation as being closer to one end of a spectrum or the other

Seven factors

- Severity
- Immediacy
- Directness
- Invasiveness
- Measurability
- Presumptive legitimacy
- Responsibility

For each factor, Schmitt

- Provides a
  - Brief description of the importance or distinctiveness of the factor
  - Formulation of questions that would satisfy the requirements of the factor
  - Vertical scale of the factor itself, divided into three broad bands to allow for
    - One each for relatively clear cases of each qualitative choice
    - A central "gray" area for factually uncertain determinations

A closer look at one factor

Presumptive Legitimacy

In most cases, whether under domestic or international law, the application of violence is deemed illegitimate absent some specific exception such as self-defense. The cognitive approach is prohibitory. By contrast, most other forms of coercion—again in the domestic and international sphere—are presumptively lawful, absent a prohibition to the contrary. The cognitive approach is permissive. Thus, the consequences of armed coercion are presumptively impermissible, whereas those of other coercive acts are not (as a very generalized rule).†

Action Accomplished by Means of Kinetic Attack
Action Accomplished in Cyberspace but Manifested by a "Smoking Hole" in Physical Space
Action Accomplished in Cyberspace and Effects Not Apparent in Physical World

Has this type of action achieved a customary acceptance within the international community?

Is the means qualitatively similar to others presumed legitimate under international law?

† Michael N. Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, 37 COLUM. J. TRANSNAT'L L. 887 (1999) at 914-15.

Scenario

- Terrorist attack on the Washington Metro (subway system in Washington, D.C.) during rush hour
- Terrorists are citizens of countries with which the U.S., at the time of the attack, is nominally at peace
- Attack orchestrated from outside the U.S. by using compromised administrative computers (used by Metro officials to monitor operations)

Use of a cyber weapon

- The terrorists use malicious code to strike the software-intensive automatic train protection (ATP) system of the Metro
  - Changes to ATP system permitted the train control system to allow
    - Two head-on train collisions
    - Three rear-end train collisions

Severity

- Crashes resulted in
  - Halting train traffic system-wide
  - Redirecting traffic from other modes
  - Thirty passengers killed
  - Over 200 passengers physically injured
  - An underdetermined number of people experienced psychological effects
  - Property damage was extensive (e.g., rail infrastructure)
  - Significant loss of intangible property (e.g., expenditure of considerable resources to track down and remove vulnerabilities of the system that were exploited by the terrorists)

Immediacy

- Duration of attack was two minutes
- Effects of attack are tiered:
  - Instantaneous: crashes themselves
  - System shut down after ten minutes
  - Many people avoided using mass transportation for sometime thereafter
  - Partial reopening of system after two weeks, with return to full operation after several months

Directness

- Software was used to cause the disturbance in the Metro system
- The attack represents a specific break-in
  - One act had one effect

Invasiveness

- Locus of the attack was solely in the U.S.

Measurability

- Effect of the attack can be quantified to some extent
- Nonphysical effects (e.g., loss of public confidence in the Metro system) are difficult to quantify

Presumptive legitimacy

- No one can launch this type of attack—not even nation states—against noncombatants

Responsibility

- No countries claimed responsibility for the attack
- However, we can apply the legal principle of *res ipsa loquitur*
  - Assume that the injury to the passengers was caused by the negligent action of another party because the trains collisions are of the sort that would not occur unless some party acted in a negligent manner

Consequences

	Numeric rating
Severity	8
Immediacy	9
Directness	9
Invasiveness	5
Measurability	9
Presumptive legitimacy	5
Responsibility	5
Total	50
Simple average	7.1

Need for weighting

- Primary analysis is fact driven
  - Facts from the operator and no legal judgment—collect legally operative facts
- Secondary analysis involves the attorney weighting each of the seven factors for the fact pattern

Discussion

- Severity of attack is comparable to that of the September 11, 2001 attack on the World Trade Center
- Attack is extreme in both aspects of invasiveness, but lower for the intangible aspects and distance from the target

Overall assessment

- Place the consequences of the attack in the low end of the high range of the Schmitt scale
- Can conclude that an armed attack occurred
  - Both the UN Article 2(4) (i.e., use of force) and UN Article 51 (i.e., self defense) thresholds were crossed, portending a movement toward conflict between the aggressor and the U.S.

Caveat

- Schmitt Analysis is intended for performing an academically rigorous evaluation of the factors affecting a lawful response to a terrorist attack
  - It not meant to be applied as a mechanical algorithm
- We did not weight the factors in our example, but would do so in a real analysis

Conclusion

- With appropriate training, information, and analysis, it will be possible to apply Schmitt Analysis to
  - Reduce the "gray area" of legal uncertainty to an absolute minimum
  - Allow the most complete range of effective responses against those who attack a nation's critical infrastructure

Contact information

- bmichael@nps.navy.mil
- twingfield@potomacinstitute.org

- Papers on this topic can be found at

http://www.cs.nps.navy.mil/people/faculty/bmichael/